

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS  
COUNTY DEPARTMENT, CHANCERY DIVISION

JAMEL BARNES, individually and on behalf  
of all others similarly situated,

*Plaintiff,*

v.

ARYZTA, LLC, a Delaware limited liability  
company,

*Defendant,*

and

AUTOMATIC DATA PROCESSING, INC., a  
Delaware corporation,

*Respondent In Discovery.*

Case No.:

**CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Jamel Barnes brings this Class Action Complaint and Demand for Jury Trial against Defendant Aryzta, LLC to put a stop to its unlawful collection, use, and storage of Plaintiff's and the proposed Class's sensitive biometric data. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

**NATURE OF THE ACTION**

1. Defendant Aryzta is a leading global supplier of baked foods for the foodservice, retail, and restaurant industries. In the United States, Aryzta is best known for its Otis Spunkmeyer and La Brea Bakery brands. In order to produce and sell its baked products, Aryzta employs a wide range of individuals throughout the world, including at its facilities located in the State of Illinois.

2. When employees first begin their jobs at Aryzta, they are required to scan their fingerprint in its time clocks. That's because Aryzta uses a biometric time tracking system that requires employees to use their fingerprint as a means of authentication, instead of key fobs or identification cards.

3. While there are tremendous benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with the employee. This exposes employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed, employees have no means by which to prevent identity theft and unauthorized tracking.

4. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), specifically to regulate companies that collect and store Illinois citizens’ biometrics, such as fingerprints.

5. Despite this law, Aryzta disregards its employees’ statutorily protected privacy rights and unlawfully collects, stores, and uses their biometric data in violation of the BIPA. Specifically, Aryzta has violated (and continues to violate) the BIPA because it did not (and continues not to):

- Properly inform Plaintiff and the Class members in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, and used, as required by the BIPA;
- Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff’s and the Class’s fingerprints, as required by the BIPA; nor
- Receive a written release from Plaintiff or the members of the Class to collect, capture, or otherwise obtain their fingerprints, as required by the BIPA.

6. Accordingly, this Complaint seeks an Order: (i) declaring that Defendant’s

conduct violates BIPA; (ii) requiring Defendant to cease the unlawful activities discussed herein; and (iii) awarding liquidated damages to Plaintiff and the proposed Class.

### **PARTIES**

7. Plaintiff Jamel Barnes is a natural person and citizen of the State of Illinois.

8. Defendant Aryzta, LLC is a limited liability company existing under the laws of the State of Delaware. Aryzta is registered to conduct business with the Illinois Secretary of State (File No. 03527557). Aryzta conducts business throughout this County, the State of Illinois, and the United States.

9. Respondent In Discovery Automatic Data Processing, Inc. ("ADP") provides Defendant Aryzta human resource management software and services, including employee time tracking services. As such, Plaintiff believes that ADP possesses information essential to the determination of who should properly be named as additional defendants in this action. For instance, Plaintiff believes that ADP possesses information that can identify additional individuals or entities that may have collected, used, and stored Plaintiff's and the proposed Class's sensitive biometric data.

### **JURISDICTION AND VENUE**

10. This Court has jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because Defendant conducts business transactions in Illinois, has committed tortious acts in Illinois, and is registered to conduct business in Illinois.

11. Venue is proper in Cook County because Defendant maintains offices in Cook County and conducts business transactions in Cook County.

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 3 of 16

## FACTUAL BACKGROUND

### I. The Biometric Information Privacy Act.

12. In the early 2000's, major national corporations started using Chicago and other locations in Illinois to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing, yet unregulated technology. *See* 740 ILCS 14/5.

13. In late 2007, a biometrics company called Pay by Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

14. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information", Illinois enacted the BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

15. The BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 4 of 16

trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it *first*:

- (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
- (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
- (3) receives a written release executed by the subject of the biometric identifier or biometric information.”

740 ILCS 14/15(b).

16. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a “written release” specifically “in the context of employment [as] a release executed by an employee as a condition of employment.” 740 ILCS 14/10.

17. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and—most importantly here—fingerprints. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *See id.*

18. The BIPA also establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS 14/15(c)–(d). For instance, the BIPA requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

19. Ultimately, the BIPA is simply an informed consent statute. Its narrowly tailored

provisions place no absolute bar on the collection, sending, transmitting or communicating of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be collected, sent, transmitted, or stored. The BIPA simply mandates that entities wishing to engage in that conduct must put in place certain reasonable safeguards.

## **II. Defendant Violates the Biometric Information Privacy Act.**

20. By the time the BIPA passed through the Illinois Legislature in mid-2008, many companies who had experimented using biometric data as an authentication method stopped doing so. That is because Pay By Touch's bankruptcy, described in Section I above, was widely publicized and brought attention to consumers' discomfort with the use of their biometric data. Despite the recognized dangers of using biometric data in the private sector, employers have failed to follow retailers' leads in dropping it as an identification method. In fact, many employers now require their employees to register their biometric data, viewing it as a cost-effective method of authentication.

21. Unfortunately, Arysza failed to take note of the retail industry's trend recognizing the dangers in storing biometric identifiers and the passage of Illinois law governing the collection and use of biometric data. Arysza continues to collect, store, and use its employees' biometric data in violation of the BIPA.

22. Specifically, when employees first begin work at Arysza, they are required to have their fingerprint scanned in order to enroll them in Arysza's fingerprint database.

23. Arysza uses an employee time tracking system that requires employees to use their fingerprint as a means of authentication. Unlike a traditional time clock, employees have to use their fingerprints to "punch" in to or out of work.

24. Unfortunately, Arysza fails to inform its employees the extent of the purposes for which it collects their sensitive biometric data or to whom the data is disclosed, if at all.

25. Arysza similarly fails to provide its employees with a written, publicly available policy identifying its retention schedule, and guidelines for permanently destroying its employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by the BIPA. An employee who leaves the company does so without any knowledge of when their biometric identifiers will be removed from Arysza's databases—or if they ever will be.

26. The Pay By Touch bankruptcy that catalyzed the passage of the BIPA highlights why conduct such as Arysza's—where employees are aware that they are providing biometric identifiers but are not aware of to whom or the full extent of the reasons they are doing so—is so dangerous. That bankruptcy spurred Illinois citizens and legislators into realizing a critical point: it is crucial for people to understand when providing biometric identifiers who exactly is collecting their biometric data, where it will be transmitted to, for what purposes, and for how long. But Arysza disregards these obligations, and instead unlawfully collects, stores, and uses its employees' biometric identifiers and information.

27. Ultimately, Arysza not only disregards its employees' privacy rights, but it also violates BIPA.

### **III. Plaintiff Barnes's Experience.**

28. Plaintiff Barnes worked for Arysza at its Romeoville, Illinois facility from May 2014 to September 2015.

29. As a new employee, Plaintiff was required to scan his fingerprint so that Arysza could use it as an authentication method to track his time.

30. Aryzta subsequently stored Barnes's fingerprint data in its databases.

31. Each time Barnes began and ended his workday he was required to scan his fingerprint.

32. Barnes has never been informed of the specific limited purposes or length of time for which Aryzta collected, stored, or used his fingerprints.

33. Barnes has never been informed of any biometric data retention policy developed by Aryzta, nor has he ever been informed of whether Aryzta will ever permanently delete his fingerprints.

34. Barnes has never been provided with nor ever signed a written release allowing Aryzta to collect or store his fingerprints.

35. Barnes has continuously and repeatedly been exposed to the risks and harmful conditions created by Aryzta's violations of the BIPA alleged herein.

36. As a result of Aryzta's conduct, Barnes has experienced bodily injury in the form of mental anguish. For example, Barnes experiences mental anguish and injury when thinking about what would happen to his biometric data if Aryzta went bankrupt, whether Aryzta will ever delete his biometric information, and whether (and to whom) Aryzta shares his biometric information.

37. Barnes seeks liquidated damages under BIPA as compensation for the injuries Aryzta has caused.

#### CLASS ALLEGATIONS

38. **Class Definition:** Plaintiff Barnes brings this action pursuant to 735 ILCS 5/2-801 on behalf of himself and a class of similarly situated individuals, defined as follows:

All residents of the State of Illinois who had their fingerprints collected, captured, received, otherwise obtained, or disclosed by Aryzta while residing in Illinois.



The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

39. **Numerosity:** The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from at least hundreds of employees who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

40. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

- a) whether Arysza collected, captured, or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;
- b) whether Arysza properly informed Plaintiff and the Class of its purposes for collecting, using, and storing their biometric identifiers or biometric information;
- c) whether Arysza obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's and the Class's biometric identifiers or biometric information;

- d) whether Aryzta has disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information to any third parties;
- e) whether Aryzta has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;
- f) whether Aryzta developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever occurs first;
- g) whether Aryzta complies with any such written policy (if one exists);
- h) whether Aryzta used Plaintiff's and the Class's fingerprints to identify them; and
- i) whether Aryzta's violations of the BIPA were committed negligently.

41. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

42. **Appropriateness:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could

sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

**FIRST CAUSE OF ACTION**  
**Violation of 740 ILCS 14/1, *et seq.***  
**(On Behalf of Plaintiff and the Class)**

43. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

44. The BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, the BIPA makes it unlawful for any private entity to “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers or biometric information, unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; *and* (3) receives a written release executed by the subject of the biometric identifier or biometric information...” 740 ILCS 14/15(b) (emphasis added).

45. The BIPA also prohibits private entities from disclosing a person’s biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

46. The BIPA also mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention (and—importantly—deletion) policy.

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 11 of 16

Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (i.e., when the employment relationship ends); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

47. Unfortunately, Arysza fails to comply with these BIPA mandates.

48. Arysza is a limited liability company and thus qualifies as a “private entity” under the BIPA. *See* 740 ILCS 14/10.

49. Plaintiff and the Class are individuals who had their “biometric identifiers” collected by Arysza (in the form of their fingerprints), as explained in detail in Section II. *See* 740 ILCS 14/10.

50. Plaintiff’s and the Class’s biometric identifiers were used to identify them, and therefore constitute “biometric information” as defined by the BIPA. *See* 740 ILCS 14/10.

51. Arysza violated 740 ILCS 14/15(b)(3) by negligently failing to obtain written releases from Plaintiff and the Class before it collected, used, and stored their biometric identifiers and biometric information.

52. Arysza violated 740 ILCS 14/15(b)(1) by negligently failing to inform Plaintiff and the Class in writing that their biometric identifiers and biometric information were being collected and stored.

53. Arysza violated 740 ILCS 14/15(b)(2) by negligently failing to inform Plaintiff and the Class in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored, and used.

54. Arysza violated 740 ILCS 14/15(a) by negligently failing to publicly provide a retention schedule or guideline for permanently destroying its customers’ biometric identifiers

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 12 of 16

and biometric information.

55. By negligently collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Arysza violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in the BIPA, 740 ILCS 14/1, *et seq.*

56. On behalf of himself and the Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Arysza to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) liquidated damages of \$1,000 per violation for each of Arysza's negligent violations of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

**SECOND CAUSE OF ACTION**  
**Negligence**  
**(On Behalf of Plaintiff and the Class)**

57. Plaintiff incorporates the foregoing allegations as is fully set forth herein.

58. Arysza owed Plaintiff a duty of reasonable care. That duty required that Arysza exercise reasonable care in the collection and use of Plaintiff's biometric identifiers or biometric information. Specifically Arysza was required to collect, retain, store, and use Plaintiff's and the Class's biometric information and identifiers in compliance with the standards set forth by the BIPA.

59. Additionally, Arysza owed Plaintiff a heightened duty—under which Arysza assumed a duty to act carefully and not put Plaintiff at undue risk of harm—because of the employment relationship of the Parties.

60. Arysza breached its duties by failing to implement reasonable procedural

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 13 of 16

safeguards around the collection and use of Plaintiff's biometric identifiers and biometric information.

61. Specifically, Arysza breached its duties by failing to properly inform Plaintiff in writing of the specific purpose or length of time for which his fingerprints were being collected, stored, and used.

62. Arysza also breached its duties by failing to provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's fingerprints.

63. Arysza's breach of its duties proximately caused and continues to cause Plaintiff mental anguish and mental injury. For example, Plaintiff experiences mental anguish when thinking about what would happen to his biometric identifiers or information if Arysza went bankrupt, whether Arysza will ever delete his biometric identifiers or information, and whether (and to whom) Arysza shares his biometric identifiers or information.

64. Accordingly, Plaintiff seeks an order declaring that Arysza's conduct constitutes negligence, and awarding Plaintiff and the Class damages in an amount to be calculated at trial.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff Barnes, on behalf of himself and the Class, respectfully requests that this Court enter an Order:

- A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Barnes as representative of the Class, and appointing his counsel as Class Counsel;
- B. Declaring that Arysza's actions, as set out above, violate the BIPA;
- C. Awarding statutory damages of \$1,000 for each of Defendant's violations of the BIPA, pursuant to 740 ILCS 14/20(1);

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 14 of 16

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including an Order requiring Aryzta to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Declaring that Aryzta's actions, as described above, constitute negligence;

F. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as equity and justice may require.

#### **JURY TRIAL**

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

**JAMEL BARNES**, individually and on behalf of  
all others similarly situated,

Dated: August 17, 2017

By: s/Benjamin H. Richman  
One of Plaintiff's Attorneys

Jay Edelson  
jedelson@edelson.com  
Benjamin H. Richman  
brichman@edelson.com  
Sydney Janzen  
sjanzen@edelson.com  
EDELSON PC  
350 North LaSalle Street, 13th Floor  
Chicago, Illinois 60654  
Tel: 312.589.6370  
Fax: 312.589.6378  
Firm ID: 44146

David Fish  
dfish@fishlawfirm.com  
John Kunze

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 15 of 16

jkunze@fishlawfirm.com  
THE FISH LAW FIRM, P.C.  
200 East Fifth Avenue, Suite 123  
Naperville, Illinois 60563  
Tel: 630.355.7590  
Fax: 630.778.0400  
Firm ID: 44086

ELECTRONICALLY FILED  
8/17/2017 4:39 PM  
2017-CH-11312  
PAGE 16 of 16